В настоящее время участились случаи заражения компьютеров опасным вирусом, фактически, уничтожающим все данные пользователей. Это, так называемый «вирус-шифровальщик» или «вирус-вымогатель». **Особенно опасной эту угрозу делает тот факт, что далеко не все антивирусы способны предотвратить ущерб от действия данного вида вредоносных программ. Наиболее надежной защитой является осторожность и внимательность самого пользователя.** В связи с этим предлагается ознакомиться с данным материалом, описывающим принцип действия таких вирусов и методы борьбы с ним.

Приведенный в действие вирус сканирует жесткий диск компьютера и все доступные носители информации (подключенные флешки, внешние жесткие диски, карты памяти и т.д.), отыскивая определенные категории файлов. Как правило, это файлы, с наибольшей вероятностью содержащие ценную для пользователя информацию: текстовые документы, фотографии, электронные таблицы, архивы, базы данных 1С, рабочие файлы различных программ и т.д. Далее все обнаруженные файлы шифруются одним из видов крипотустойчивых алгоритмов. Для пользователя это означает две неприятные вещи:

1. Все его личные и рабочие файлы невозможно открыть и как-либо использовать, так как они зашифрованы;
2. Расшифровать файлы, не зная ключа (т.е. взломать шифр), невозможно.

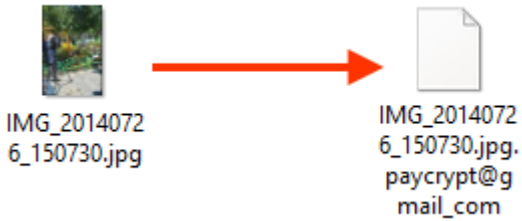

Рисунок 1 - Исходный (слева) и зашифрованный (справа) файл

Вирус-шифровальщик отличается тем, что, как правило, не пытается «пролезть» в компьютер пользователя, используя системные уязвимости. Он использует для этого самого пользователя. Наиболее вероятный сценарий – вредоносный файл приходит по электронной почте. Причем электронное письмо, скорее всего, будет тщательно замаскировано под важную для пользователя информацию. Например, оно может называться «Повестка в суд», «Акт выполненных работ», «Уведомление о задолженности», «Изменения в налоговом кодексе РФ» и т.д. и т.п. Наиболее опасными являются не автоматически сгенерированные по определенному шаблону письма, а отправленные специально и конкретному лицу. В этом случае злоумышленник может подобрать наиболее правдоподобное для вас содержание письма, с учетом ваших персональных данных и должности. В любом случае подобные послания преследуют ровно одну цель: под видом важной информации подсунуть исполняемый файл в приложении или ссылку на его скачивание. При открытии такого файла пользователем запускается вирус. Нередко параллельно с вирусом запускается также и текстовый документ, содержащий информацию по теме письма, просто для того чтобы усыпить внимание. Пока пользователь читает документ, вредоносная программа шифрует данные на компьютере.

1. **Следует с подозрением относится к любым письмам со ссылками и вложенными файлами. Прежде всего, нужно обращать внимание на адрес отправителя. Если адрес выглядит примерно так «darryl.rosenberg@gic-web-bsd-033.genotec.ch» то это явно никакое не официальное письмо, а послание от спамера/хакера. Однако вредоносные файлы могут приходить и с вполне благонадежных на вид**

адресов, на сегодняшний день вполне возможно подделать электронный адрес отправителя до степени смешения с почтой официальных учреждений.

2. **При получении письма с вложенными файлами обращайте внимание на расширение файлов! Это очень важно, так как вирус стараются маскировать под текстовые документы или аудио-видео записи. При этом во вложении, как правило, отображается полное расширения файла, в результате у файла оказывается «двойное» расширение, например: имя_файла.docx.bat (см. рис. 2 и рис.3) В данном случае docx – это формат документа MS Word. Именно под него маскируется файл. А истинное расширение – bat. Это формат исполняемого файла, который может содержать вредоносный код. При попытке открыть такой «документ» вы можете своими руками запустить на компьютер вирус. Поэтому никогда не скачивайте из электронной почты файлы, если на конце отображается одно из следующих расширений: .exe, .com, .js, .wbs, .hta, .bat, .cmd, .msi.**

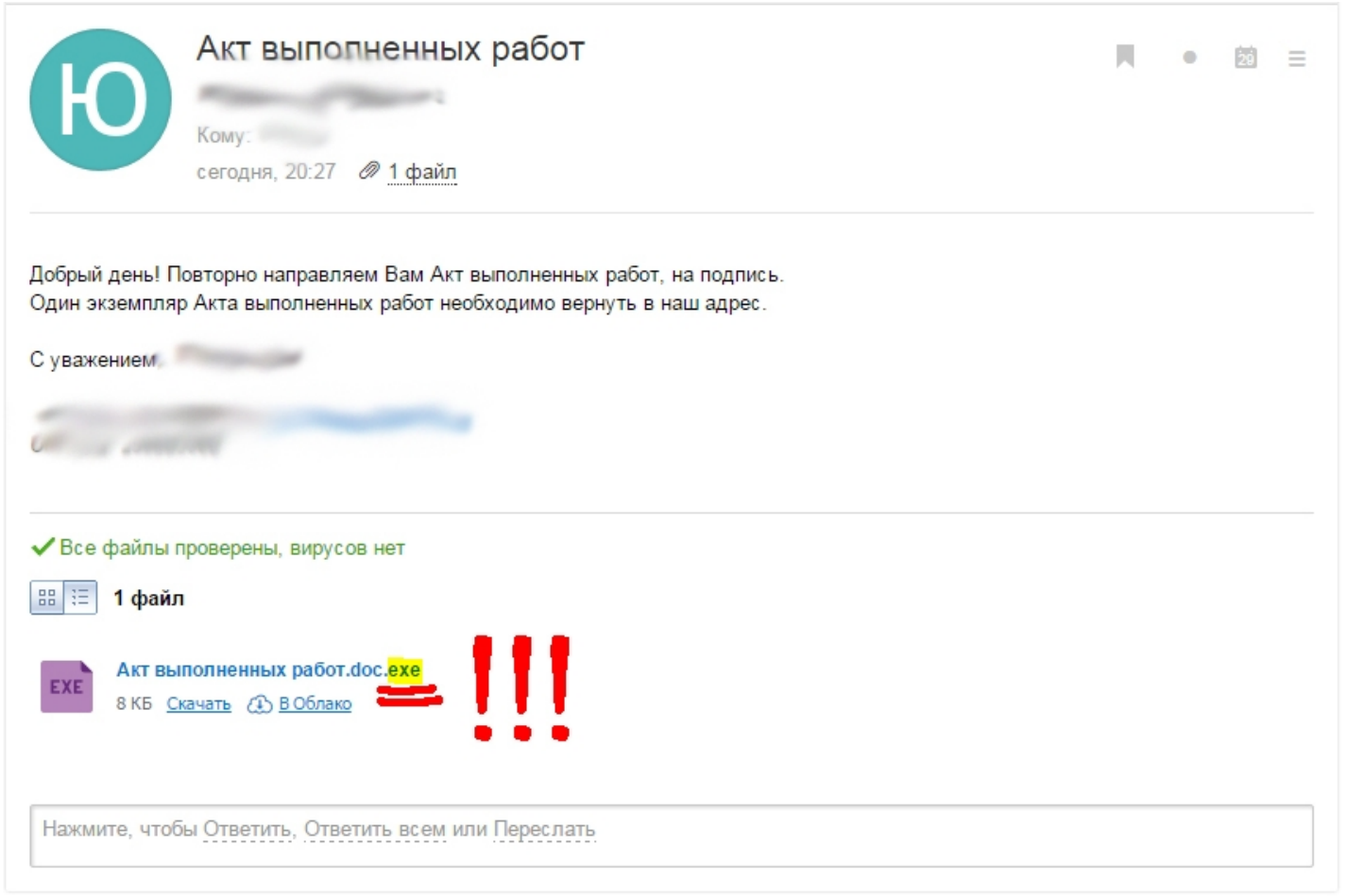

*Рисунок 2 - Во вложении файл с расширением **.exe** замаскированный под документ MS Word*

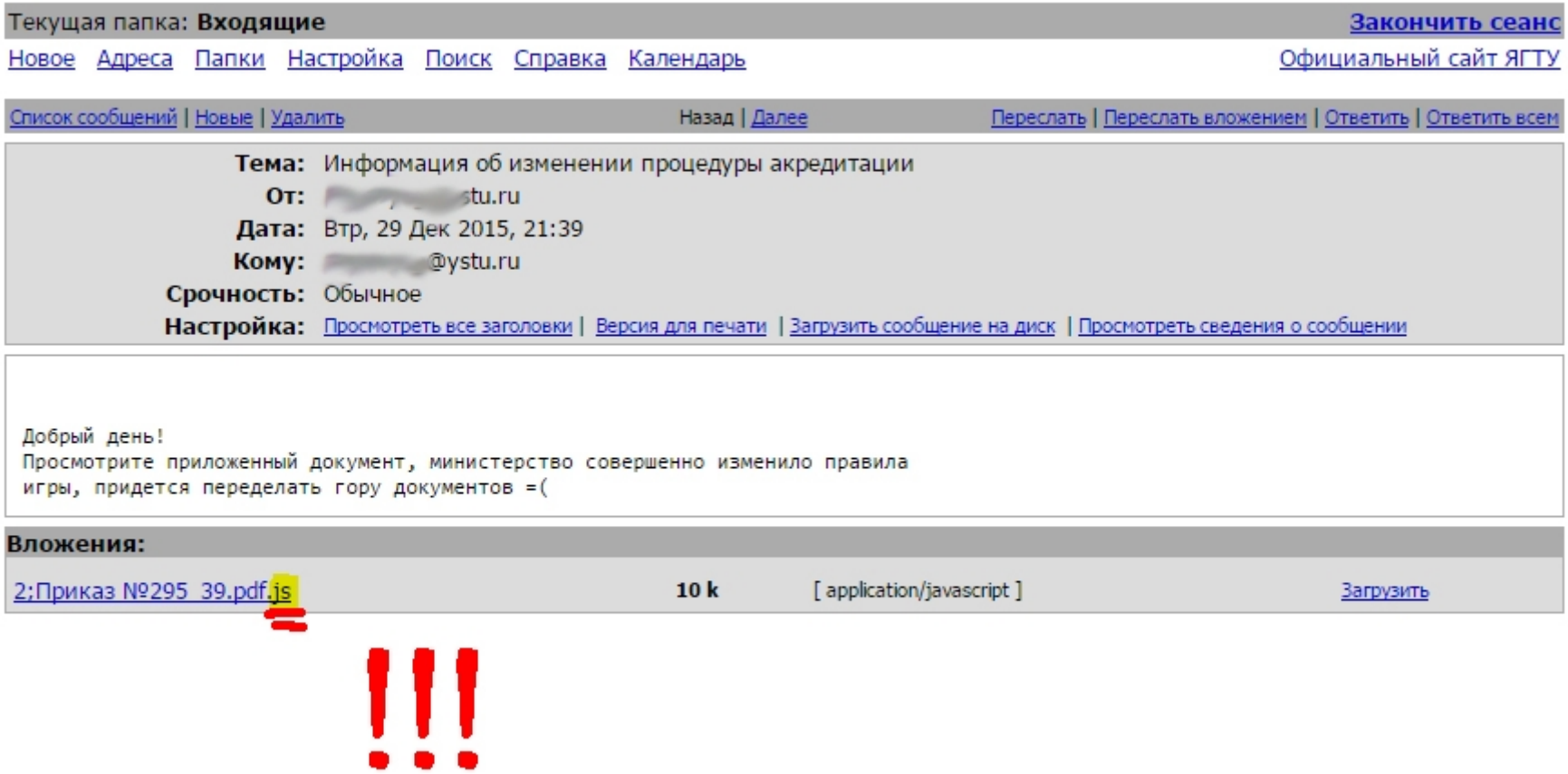

*Рисунок 3 - Во вложении файл с расширением **.js** замаскированный под pdf-документ*

3. Во вложении может находиться безобидный на вид архив или же ссылка на скачивание файла. При этом распаковав архив или скачав файл по ссылке вы можете не заметить «истинную сущность» файла, так как во многих операционных системах расширения файлов могут быть скрыты. Поэтому необходимо включить их отображение и следить за форматом открываемых документов. Для этого выполните следующие действия:

   а) **Если у вас Windows 8/Windows 8.1:**
   Наверху открытого окна перейти на вкладку «Вид» и установить галочку напротив «Расширения имен файлов»

   б) **Если у вас Windows 7:**
   На клавиатуре нажать левый Alt. Наверху появится главное меню (рис.4).

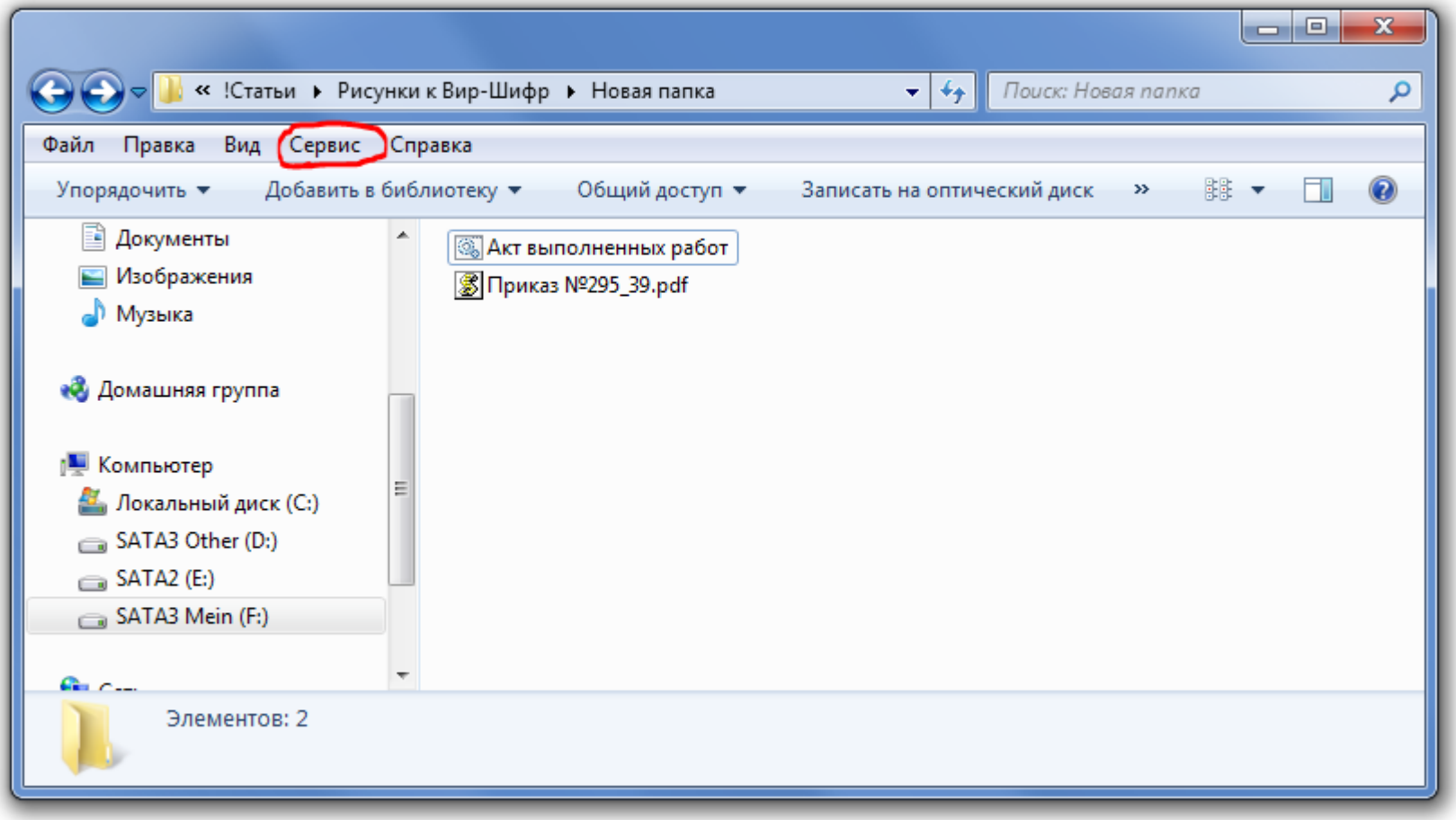

Рисунок 4 - Нажмите Alt на клавиатуре и в появившемся в верхней части окна меню выберите «Сервис». Далее в выпадающем меню нажмите строку «Параметры папок»

В нем открыть меню «Сервис – Параметры папок». В открывшемся окне перейти на вкладку «Вид». В списке дополнительных параметров почти в самом низу снять галочку напротив «Скрывать расширения для зарегистрированных типов файлов» и нажать кнопку «ОК» или «Применить» (рис.5).

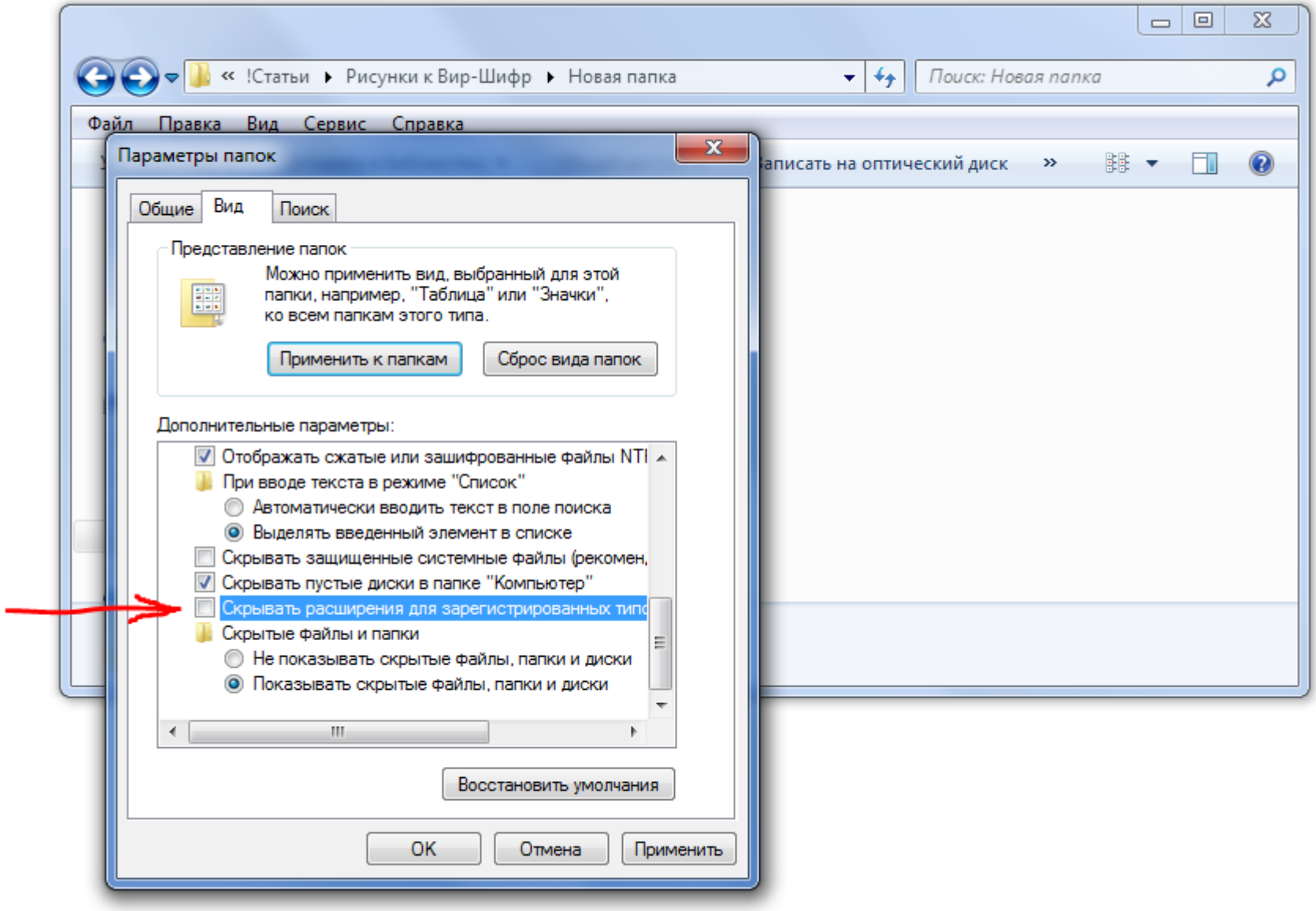

Рисунок 5 - В параметрах папок выберите вкладку «Вид» и снимите галочку «Скрывать расширения для зарегистрированных типов файлов».

в) **если у вас Windows XP:**

Все аналогично Windows 7 за исключением нажатия кнопки Alt для вызова главного меню. Оно обычно всегда отображается в Windows XP.

После выполнения данных операций в вашей системе будут отображаться расширения файлов (рис.6).

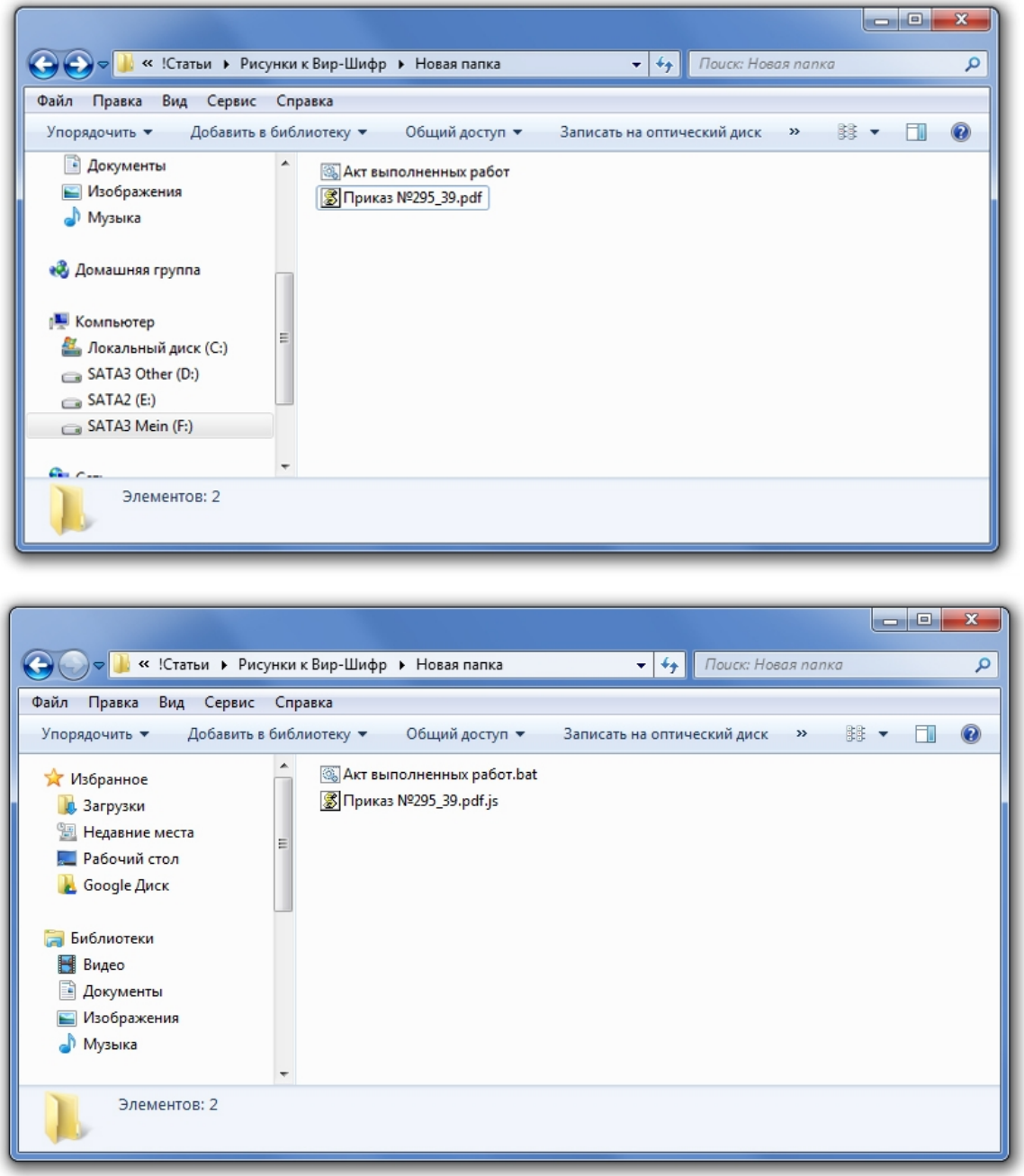

Рисунок 6 - Сверху – расширения файлов скрыты. В папке два документа, по внешнему виду которых трудно понять, что это вредоносные программы. Внизу – расширения файлов отображаются, при этом видно, что у первого файла расширение .bat, а второй только маскировался под pdf-файл, а на самом деле это скрипт с расширением .js

4. Если вы все же скачали и запустили подозрительный файл, то операционная система может вывести на экран предупреждение примерно такого вида:

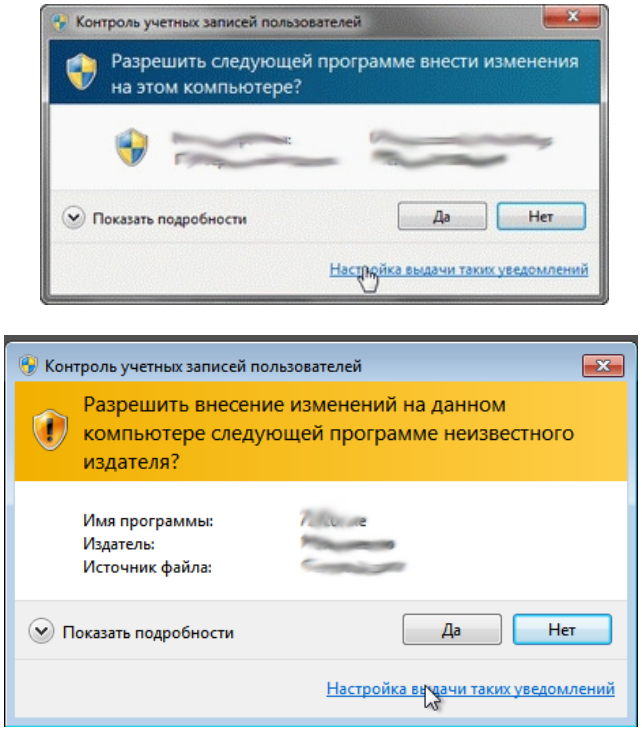

Рисунок 7 - Примерный вид предупреждающий окон Windows

Если при попытке открытия файла, полученного по электронной почте появляется такое окно, следует нажимать «НЕТ». При запуске обычных безопасных файлов откроется ассоциированная с ними программа, например Microsoft Word или Adobe Acrobat. Появление же такого окна означает, что вы пытаетесь запустить файл, который может внести изменения в систему, в т.ч. без вашего ведома, и если вы получили такой файл по электронной почте это на 95% вирус.

Также следует помнить, что такое окно может и не высветиться при открытии вредоносного файла.

Угроза подобных вирусов, распространяющихся через электронную почту весьма велика. За последний год более 300 крупных фирм и компаний по всему миру пострадали от этого вида угроз.